* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]this invention relates to the art of attestation in case communication between 2 devices which turn into the attestation side device and an attesting side device especially is performed via the 3rd device about the art which attests the justification of a communications partner.
[0002]
[Description of the Prior Art]As art which attests the justification of a communications partner, the authentic method using an unsymmetrical key cryptosystem specified in ISO (ISO9798-3) is known, for example.
[0003]As an authentic method using an unsymmetrical key cryptosystem, two methods, one-pass attestation and two pass attestation, are known.
[0004]In one-pass attestation, the side attested enciphers what added the near identifier, time stamp, or consecutive numbers attested by the plaintext using its secret key. The side to attest decrypts using the public key which becomes a secret key which receives the cryptogram, and in which the side attested has it, and a pair, and attests by performing the check of an identifier, a time stamp, or consecutive numbers.
[0005]In two pass attestation, the side attested receives a random number from the side to attest, and enciphers the identifier of the side attested with this random number using a secret key. The side to attest receives the cryptogram, decrypts using the public key corresponding to the secret key of the side attested which it has, and attests by checking an identifier and a random number.
[0006]As art which attests the justification of a communications partner, the authentic method using a symmetrical key cryptosystem specified to ISO (ISO9798-2) is also known.
[0007]in addition, as art which attests the justification of a communications partner, as the art which does not need an enciphering function for the side attested -- " -- international standard detailed-explanation "main point of EMV standard specifications" EMV of a financial system IC card -- in order to understand standard foundations and application --";

Nishizaki ****** As indicated without SHIMEDIA pp.62-pp.67, The static authentic method specified to EMV is known.

[0008]In this static attestation, the side attested holds a plaintext, the cryptogram acquired by enciphering a plaintext with a secret key, and the public key which become that secret key and pair and which the certificate authority attested. The side to attest receives the plaintext, a cryptogram, and a public key, and attests by decrypting a cryptogram using a public key and investigating compatibility with a plaintext.

[0009]

[Problem(s) to be Solved by the Invention]Communication between 2 devices may be performed via the 3rd device.

[0010]For example, the electronic fee collection sytem (ETC) system of a toll road comprises an IC card which a user possesses for every user, a mounted vessel carried in each car fixed for every car, and a road-side machine installed in the tollgate for every tollgate, and an IC card and a road-side machine communicate via a mounted vessel. In such an ETC system, a user inserts the self IC card to possess in the mounted vessel carried by the car at the time of automobile boarding. And when a car passes through a tollgate nonstop, the road-side machine installed in the tollgate charges a fee at the IC card inserted in the mounted vessel carried in the car which passes through a tollgate. In this case, it is necessary to attest between the IC card which performs such electronic settlement processing, and a road-side machine.

[0011]If the unjust possibility of the 3rd device is taken into consideration in this way here when communicating via the 3rd device, it is insufficient to apply the art of said attestation and just to attest between an IC card and a road-side machine. For example, it is because a mounted vessel cannot deny a possibility of having become completely about operation of an IC card or a road-side machine.

[0012]Then, this invention makes it SUBJECT to provide the authentication system which can perform reliable attestation between 2 devices which communicate via the 3rd device, when communication between 2 devices is performed via the 3rd device.

[0013]By the way, since the hour corresponding given to communication between the 3rd device and one device is a short time when performing communication between 2 devices via the 3rd device, attesting may become difficult between 2 devices which communicate via the 3rd device.

[0014]For example, if the communication capability of an IC card, etc. are taken into consideration in the ETC system mentioned above, it is difficult for a car to attest between an IC card and a road-side machine between short time to pass through a tollgate nonstop.

[0015]Then, when communication between 2 devices is performed via the 3rd device still in this way, even if the hour corresponding given to communication between the 3rd device and one device is a short time, this invention, Let it be SUBJECT to provide the authentication system which can perform attestation between 2 devices which communicate via the 3rd device.

[0016]

[Means for Solving the Problem]for said SUBJECT achievement, this invention is characterized by that an information system comprises the following -- for example, With the 1st device. It is an information system which has said 1st device, the 2nd device that communicates mutually, and said 2nd device and the 3rd device that communicates mutually, and said 1st device is communication between the 1st device concerned and said 2nd device.

Transmission and reception of information for attestation between said 1st device and the 2nd device.

Said 2nd device is [in / have a means which is used for attestation between the 3rd device to said 2nd device, and the 1st device and which transmits predetermined information that said 2nd device cannot be forged, and / communication between said 1st device and the 2nd device] transmission and reception of information for attestation between said 1st device and the 2nd device.

A means to receive said predetermined information from said 1st device.

In communication between said 2nd device and the 3rd device, transmission and reception of information for attestation between said 2nd device and the 3rd device, Have a means which transmits said predetermined information on said 3rd device, and said 3rd device, A means to receive transmission and reception of information for attestation between said 2nd device and the 3rd device, and said predetermined information from said 2nd device in communication between said 2nd device and the 3rd device, and a means to perform attestation between the 3rd device and the 1st device using said predetermined information transmitted from the 2nd device.

[0017]Attestation between the 3rd device and the 1st device can be performed performing mutual recognition between the 1st device, between the 2nd device and the 2nd device, and the 3rd device, and preventing injustice of the 2nd device using predetermined information that said 2nd device cannot further be forged according to such an information system. and -- in this way, between two devices each, by attesting mutually, it can have high reliability and each device can be attested with a gestalt into which injustice of other devices does not enter -- a result -- the 3rd device and the 1st -- attestation between devices can be attested with high reliability.

[0018]By being made to perform communication between said 1st device and the 2nd device in advance of communication between said 2nd device and the 3rd device in such an information system, Since transmission of said predetermined information can be performed in advance of communication between said 2nd device and the 3rd device among authenticating processings which the 1st device should perform for attestation between the 1st device and the 3rd device, Even if hour corresponding between said 2nd device and the 3rd device is not a long time so that the 1st device can perform all the authenticating processings to within a time [this], attestation between the 1st device and the 3rd device can be performed.

[0019]

[Embodiment of the Invention]Hereafter, the embodiment of this invention is described.

[0020]First, a 1st embodiment is described.

[0021]The composition of the authentication system concerning a 1st embodiment is shown in drawing 1.

[0022]The authentication system concerning a 1st embodiment comprises the certificate authority 231 which performs justification attestation of a key, IC card 201 which each driver owns, the mounted vessel 211 carried in a car, and the road-side machine 221 installed in a toll road so that it may illustrate.

[0023]IC card 201 comprises MPU202, storage device 203, and transceiver I/F204. The mounted vessel 211 comprises MPU212, the storage device 213, transceiver I/F215, and 216. The road-side machine 221 comprises MPU222, storage device 223, and transceiver I/F225.

[0024]IC card 201 and the mounted vessel 211 communicate via transceiver I/F204 and transceiver I/F215, and the mounted vessel 211 and the road-side machine 221 communicate via transceiver I/F216 and transceiver I/F225. Here, by this embodiment, IC card 201 and the mounted vessel 211 explain a cable, the mounted vessel 211, and the road-side machine 221 taking the case of the case where it communicates on radio. Although the graphic display was omitted, the mounted vessel 211, the road-side machine 221, and the certificate authority 231 are provided also with I/O devices, such as a display device and a speaker, respectively.

[0025]Next, the contents stored in the storage device 203 in IC card 201 are shown in drawing 2.

[0026]Card ID311 which is a peculiar identifier for every IC card at the storage device 203 so that it may illustrate, the ICC individual key 312 peculiar to card ID which is keys of a symmetrical cryptosystem, and the ICC peculiar secret key 313 peculiar to card ID which is secret keys of an asymmetric cipher system, . Were attested by the certificate authority 231. The ICC certificate 315, the public key 316 of a certificate authority, the counter 317, and the channel information 318 which show the justification of IC card 201 attested by the attested ICC peculiar public key 314 which are the ICC peculiar secret key 313 and a pair of public key, and the certificate authority 231 are stored. The counter 317 is a value updated for every settlement of accounts. The channel information 318 expresses the utilized route of the toll road of the car in which the mounted vessel 211 with which IC card 201 was inserted was carried, and is updated according to operation of cars. Here, the attested ICC peculiar public key 314 and the ICC certificate 315 are the public keys of a certificate authority, respectively, and the justification of the contents can verify them.

[0027]The various programs executed by MPU202 are stored in the storage device 203. As these programs, there is a program which realizes the authenticating processing 301, the message encryption communication processing 302, the encryption/decoding processing

303 of a symmetrical cryptosystem, the encryption/decoding processing 304 of an asymmetric cipher system, and attestation child generation processing 305 as a process by execution of MPU202.

[0028]Next, the contents stored in the storage device 213 of the mounted vessel 211 are shown in drawing 3.

[0029]. Were attested by peculiar mounted vessel ID411 which is an identifier, the mounted vessel individual key 412 which it is peculiar to mounted vessel ID, and is keys of a symmetrical cryptosystem, the mount machine [which is a secret key of an asymmetric cipher system] peculiar [it is peculiar to mounted vessel ID, and] secret key 413, and the certificate authority 231 for every mounted vessel at the storage device 213 so that it might illustrate. The attested mount machine peculiar public key 414 which are the mounted vessel peculiar secret key 413 and a pair of public key, and the public key 415 of the certificate authority are stored. Here, the attested mount machine peculiar public key 414 is a public key of a certificate authority, and the justification of the contents can verify it.

[0030]The various programs executed by MPU212 are stored in the storage device 213. As these programs, there is a program which realizes the authenticating processing 401, the message encryption communication processing 402, the encryption/decoding processing 403 of a symmetrical cryptosystem, the encryption/decoding processing 404 of an asymmetric cipher system, and attestation child generation processing 405 as a process by execution of MPU212.

[0031]Next, the contents stored in the storage device 223 of the road-side machine 221 are shown in drawing 4.

[0032]. Received attestation of peculiar road-side machine ID511 which is an identifier, the ICC individual key generation key 512, the mounted vessel individual key generation key 513, the road-side machine peculiar secret key 514 peculiar to road-side machine ID that is secret keys of an asymmetric cipher system, and the certificate authority 231 in the storage device 223 for every road-side machine so that it might illustrate. The road-side machine certificate 516 showing the justification of a road-side machine and the public key 517 of a certificate authority which were attested by the attested road-side machine peculiar public key 515 which are the road-side machine peculiar secret key 514 and a pair of public key, and the certificate authority 231 are stored. Here, the attested road-side machine peculiar public key 515 and the road-side machine certificate 516 are the public keys of a certificate authority, and the justification of the contents can verify them.

[0033]The various programs executed by MPU222 are stored in the storage device 223. As these programs, by execution of MPU222, as a process, There is a program which realizes the authenticating processing 501, the message encryption communication processing 502, the encryption/decoding processing 503 of a symmetrical cryptosystem, the encryption/decoding processing 504 of an asymmetric cipher system, the individual key generation processing 505, and attestation child generation processing 506.

[0034]Here the mounted vessel individual key generation key 513, mounted vessel ID, and a mounted vessel individual key, The individual key generation processing 505 from the mounted vessel individual key generation key 513 and mounted vessel ID. Have a relation which can generate the mounted vessel individual key corresponding to the mounted vessel ID, and the ICC individual key generation key 512, card ID, and an ICC individual key, The individual key generation processing 505 has a relation which can generate the ICC individual key generation key 512 and the ICC individual key corresponding to the card ID from card ID.

[0035]The various key information and the various certificates which are stored in the above storage devices 203, 213, and 223 are information generated, attested and managed by the certificate authority 231, beforehand, are distributed on-line or off-line, and are stored in the storage devices 203, 213, and 223. Of course, the certificate authority 231 may be constituted for every roles, such as generation, issue, and management, by two or more organizations which bear each role.

[0036]Hereafter, the authenticating processing which such an authentication system performs is explained.

[0037]This authenticating processing is processing which attests between IC card 201, the mounted vessel 211, and the road-side machine 221 of exit tollgate installation.

[0038]The procedure of authenticating processing is shown in drawing 5.

[0039]In authenticating processing, the certification information for road-side machine 221 of IC card 201, the mutual recognition of the mounted vessel 211, and IC card 201 from IC card 201 to the mounted vessel 211 is transmitted in Step 102 of IC card 201, and Step 112 of the mounted vessel 211 so that it may illustrate.

[0040]Next, in Step 113 of the mounted vessel 211, and Step 123 of the road-side machine 221 of exit tollgate installation, The mutual recognition of the mounted vessel 211 and the road-side machine 221 of exit tollgate installation, transmission of the certification information for road-side machine 221 of IC card 201 from the mounted vessel 211 to the road-side machine 221, and IC card 201 of the road-side machine 221 are attested.

[0041]In the above authenticating processing, Step 113 of the mounted vessel 211 and Step 123 of the road-side machine 221 of exit tollgate installation are performed when a car passes through a tollgate exit, but. What is necessary is just to perform Step 102 of IC card 201, and Step 112 of the mounted vessel 211 in advance of this, when IC card 201 is inserted in the mounted vessel 211.

[0042]Hereafter, the details of each step of the authenticating processing shown in drawing 5 are explained.

[0043]First, the details of processing of Step 102 of IC card 201 of drawing 5 and Step 112 of the mounted vessel 211 are explained.

[0044]A procedure with these detailed steps is shown in drawing 6.

[0045]First, if IC card 201 is inserted, the mounted vessel 211 will generate random number Ra, and will transmit random number Ra and mounted vessel ID411 to IC card 201, so that it may illustrate.

[0046]In Step 702, IC card 201 enciphers the data for C1 creation by symmetrical cryptosystem encryption / decoding processing 303 using the ICC individual key 312, and generates the cryptogram C1. The data for C1 creation sets the execution time T1 of Step 702 as the time stamp 1301 shown in drawing 7, and sets the ICC certificate 315 as the certificate 1302. Thus, an encryption result can be changed each time and by including a time stamp can show now the uniqueness and the term of validity of C1 which are coding results. The value of the counter 317, a random number, or card ID311 grade may be included in this data for C1 creation like a time stamp.

[0047]Next, IC card 201 generates the signature C2 of the data for C2 creation by asymmetric cipher system encryption / decoding processing 304 in Step 703 using ICC proper secret key 313:SICC of the asymmetry system code of IC card 201. This data for C2 creation sets the execution time T2 of Step 703 as the time stamp 1101 shown in drawing 8, The cryptogram C1 which set up random number Ra for the random number 1103, and generated mounted vessel ID at Step 702 to the signature 1104 of the ICC certificate is assigned to the attestation side intrinsic identification child 1102. Thus, an encryption result can be changed each time and by including a time stamp and a random number can show now the uniqueness and the term of validity of C2 which are coding results. The card ID311 grade of the counter 317 may be included in this data for a signature for C2 as well as a time stamp.

[0048]Next, IC card 201 generates the random number Rb, and transmits the cryptogram C1, the signature C2, the time stamp T2 used previously, card ID (ICCID), the generated random number Rb, and the attested ICC peculiar public key 314 to the mounted vessel 211. However, when the counter 317 is included in C2, the counter 317 also transmits.

[0049]The mounted vessel 211 which received these checks that the attested ICC peculiar public key 314 is correctly attested using the public key 415 of a certificate authority in Step 712, Verified ICC peculiar public key :P ICC is used and it is verified whether it is the right as a signature of the data for C2 creation which the signature C2 generated or received by asymmetric cipher system encryption / decoding processing 404. And in Step 713, if a verification result is O.K., it will progress to Step 715, and if it is not O.K., processing will be stopped in Step 714. In the case of the stop of processing, display that on the screen of the mounted vessel 211, it announces with a sound, or the ICC card 201 is discharged from the mounted vessel 211, for example.

[0050]Next, the mounted vessel 211 generates the signature C3 of the data for C3 creation by asymmetric cipher system encryption / decoding processing 404 in Step 715 using mounted vessel proper secret key 413:SOBE of the asymmetry system code of the mounted vessel 211. Execution time T3 of Step 715 is set as the time stamp 1201 of drawing 9, card ID(ICCID) 311 is assigned to the attestation side intrinsic identification child 1202, and, as for the data for C3 creation, it sets the random number Rb as the random number 1203, respectively.

[0051]Next, the mounted vessel 211 transmits C3, time stamp T3, and the attested mount machine peculiar public key (OBE public key) 414 to IC card 201.

[0052]Receive IC card 201C3 and in Step 704 first, It checks that the received attested mount machine peculiar public key 414 is correctly attested using the public key 316 of a certificate authority, Verified mounted vessel peculiar public key :P OBE is used and it is verified whether it is the right as a signature of the data for C3 creation which the signature C3 generated or received by asymmetric cipher system encryption / decoding processing 404. And in Step 705, it will end, if a verification result is O.K., and if it is not O.K., processing will be stopped in Step 706. That is told to the mounted vessel 211, and make the mounted vessel 211 display that on a screen, it is made to announce with a sound, or is made to discharge the ICC card 201 from the mounted vessel 211 in the case of a stop. Of course, as long as IC card 201 is equipped with the output device, it may be made to perform a display and an announcement from the output device.

[0053]Next, the details of Step 113 of the mounted vessel 211 of drawing 5 and Step 123 of the road-side machine 221 of exit tollgate installation are explained.

[0054]A procedure with these detailed steps is shown in drawing 10.

[0055]First, the road-side machine 221 generates the random number R4, and transmits road-side machine ID511 and the random number R4 which are an identifier of the road-side machine 221 to the mounted vessel 211.

[0056]In Step 802, the mounted vessel 211 which received this enciphers the data for C4 creation using symmetrical cryptosystem encryption / decoding processing 403 using the mounted vessel individual key 312, and generates the cryptogram C4. The data for C4 creation the random number R5 generated to random number (1) 1401 of drawing 11, Random number (2) The cryptogram C1 is set as the signature 1405 for card ID (ICCID) which received the random number R4 received from the road-side machine 211 to 1402 to the attestation side identifier 1403, and received road-side machine ID from IC card 201 to the ICC identifier 1404.

[0057]The mounted vessel 211 transmits the signature C4 to the road-side machine 221.

[0058]Next, mounted vessel ID411 which received the road-side machine 221 in Step 812, individual using the mounted vessel individual key generation key 513 -- by key generation processing 505:f, it generates, and using the generated mounted vessel individual key, the mounted vessel individual key 412 is decoded cryptogram C4, and is verified by symmetrical cryptosystem encryption / decoding processing 513. Here, a verification result will be judged to be O.K. if the random number R4 and road-side machine ID which the road-side machine 221 transmitted previously are able to be checked. In Step 815, if a verification result is O.K., it will progress to Step 813, and if it is not O.K., processing will be stopped in Step 816. In this case, display that on the screen of the road-side machine 221, it is announced with a sound, or is told to the mounted vessel 211. Display the mounted vessel 211 told this purport on the screen of the mounted vessel 211, it is announced with a sound, or discharges the ICC card 201 from the mounted vessel 211.

[0059]Next, in Step 813, the road-side machine 221 enciphers the data for C5 creation by symmetry system cryptosystem encryption / decoding processing 514 using the mounted vessel individual key restored previously, creates the cryptogram C5, and transmits to the mounted vessel 211. The data for C5 creation sets the random number R5 as random number (1) 1501 shown in drawing 12, sets the random number R4 as random number (2) 1502, and sets mounted vessel ID to the attestation side identifier 1103.

[0060]And the road-side machine 221 transmits the cryptogram C5 to the mounted vessel 211.

[0061]In Step 803, the mounted vessel 211 will decode and verify the cryptogram C5 by symmetrical cryptosystem encryption / decoding processing 404 using the mounted vessel individual key 413, if the cryptogram C5 is received. Here, a verification result will be judged to be O.K. if the random number R4 which the mounted vessel 211 transmitted, and R5 and mounted vessel ID which were generated are able to be checked first. And in Step 804, if a verification result is O.K., processing will be ended, and if it is not O.K., processing will be stopped in Step 805. In the case of a stop, tell a mounted vessel-road-side machine attestation failure to the road-side machine 221, display on the screen of the mounted vessel 211, it announces with a sound, or IC card 201 is discharged from the mounted vessel 211.

[0062]On the other hand, the road-side machine 221 verifies the cryptogram C1 in Step 814. the road-side machine 221 is individual using card ID (ICCID) which received, and the ICC individual key generation key 512 -- the ICC individual key 312 being generated and with the generated ICC individual key 312 by key generation processing 505:f. It decodes cryptogram C1 using symmetrical cryptosystem encryption / decoding processing 513, the ICC certificate 315 is taken out, and this is verified. The check of the ICC certificate is performed according to the kind of certificate. Here, since the ICC certificate is attested by the certificate authority 331, it verifies by asymmetric cipher system encryption / decoding processing 504 using the public key 517 of a certificate authority.

[0063]It means that the road-side machine 221 verifies the justification of IC card 201, the road-side machine 221 and the mounted vessel 211 perform mutual recognition, and IC card 201 and the mounted vessel 211 had performed mutual recognition by the above. Thus, mutual recognition is performed between IC card 201, between the mounted vessels 211 and the mounted vessel 211, and the road-side machine 221, and the road-side machine 221 can attest IC card 201, preventing the injustice of the mounted vessel 211 further using the information C1 kept against the mounted vessel 211. and -- in this way, between two devices each, by attesting mutually, it can have high reliability and each device can be attested with the gestalt into which the injustice of other devices does not enter -- a result -- the road-side machine 221 -- attestation of IC card 201 can be attested with high reliability.

[0064]Since transmission of the information C1 can be performed in advance of communication of the road-side machine 221 and the mounted vessel 211 among the authenticating processings which IC card 201 should perform for attestation of IC card 201 of the road-side machine 221, Even if the hour corresponding between the road-side machine 221 and the mounted vessel 211 is a short time, IC card 201 of the road-side machine 221 can be attested.

[0065]In the above processing, the data which enciphered the road-side machine certificate 516 with the ICC individual key may be included in the cryptogram C5 at Step 813, and it may transmit to the mounted vessel 211. In this case, the mounted vessel 211 also performs processing which sends the road-side machine certificate 516 enciphered at Step 803 to IC card 201. IC card 201 decrypts the received road-side machine certificate which was enciphered with an ICC individual key, and verifies the road-side machine certificate 515.

[0066]Now, in the above authenticating processings, if attestation of IC card 201 of the road-side machine 221 of exit tollgate installation is successful, Then, in this authentication system, the road-side machine 221 of exit tollgate installation receives the notice of channel information from IC card 201 via the mounted vessel 211, the fee according to this is computed, and settlement processing which charges IC card 201 is performed. Or in advance of the authentication success of IC card 201 of the road-side machine 221 of exit tollgate installation, the notice of channel information is received from IC card 201 via the mounted vessel 211, and after attestation is successful, it is made to perform settlement processing which charges IC card 201. In settlement processing, processing etc. which are notified to IC card 201 from the road-side machine 221 of exit tollgate installation of the settlement data showing the utilization charge of a toll road, etc. are performed.

[0067]Next, renewal of the channel information stored in the memory 211 of IC card 201 is explained.

[0068]The renewal of the channel information stored in the memory 211 of IC card 201, IC card 201 from the use start of a toll road to the end of settlement of the utilization charge of a toll road, The pass data notified from the road-side machine 221 installed into the utilized route of a toll road is received via the mounted vessel 211, when a car passes each road-side machine 221, and it carries out by accumulating this as channel information. the installation point of the road-side machine 221 with which pass data notified the pass data concerned -- a car -- ******** -- alias -- it expresses. The channel information just specifies the grade course which can compute the utilization charge of a toll road. Therefore, the road-side machine 221 which notifies the information for updating such channel information is installed in a toll road entrance, a junction, etc., for example.

[0069]Only when authenticating processing of drawing 5 mentioned above between the road-side machine 221 installed into the utilized route of such a toll road and the mounted vessel 211 is performed and authenticating processing is successful, it may be made to perform notice of pass data, and notified acceptance of pass data. However, Steps 102 and 103 of the authenticating processing of drawing 5 do not carry out repeating these steps with the authenticating processing performed about an exit installation road-side machine, and carrying out, since it is common.

[0070]Now, encryption communication performs here the notice of the information on the notice of pass data, the notice of the channel information mentioned above, the settlement data performed for the settlement processing mentioned above to accumulate, etc. performed between such IC card 201 and the road-side machine 221.
[0071]It is made either the gestalt which performs the code/decoding processing which performs the termination of encryption communication with the mounted vessel 211 as a gestalt of encryption communication or gestalt which does not perform the termination of encryption communication with the mounted vessel 211.
[0072]When the mounted vessel 211 performs the termination of encryption communication, Encryption communication is performed between the mounted vessel 211 and the road-side machine 221, encryption communication is performed between the mounted vessel 211 and IC card 201, or encryption communication is respectively performed between IC card 201 and the mounted vessel 211 between the mounted vessel 211 and the road-side machine 221.
[0073]When the mounted vessel 211 does not perform the termination of encryption communication, the mounted vessel 211 performs transparent relay about encryption communication, and performs encryption communication between IC card 201 and the road-side machine 221.
[0074]As mentioned above, pass data is sent to IC card 201 from the road-side machine 221 installed into the utilized route, and is sent to the road-side machine 221 of exit tollgate installation as channel information after that. Therefore, this can also be considered to be communication of the road-side machine 221 of exit tollgate installation from the road-side machine 221 installed into [utilized route] pass data. Then, it may be made to communicate by encryption communication about the road-side machine 221 of exit tollgate installation from the road-side machine 221 installed into this utilized route.
[0075]Hereafter, this encryption communication is explained.
[0076]Here, it is a case where encryption communication is performed between IC card 201 and the road-side machine 221, and explains taking the case of the case where the information from the road-side machine 221 to IC card 201 is transmitted.
[0077]The procedure of this encryption communication is shown in drawing 13.
[0078]In this case The road-side machine 221 generates a random number as a key in Step 1811 first temporarily. And the message which is the information which includes the information notified to IC card 201 from the road-side machine 221 in Step 1812 is received, MAC (Message Authentication Code) which shows the justification of a message is generated by making a key into an initial value temporarily using attestation child generation processing 506:h.
[0079]The generation method of MAC for example, ISO/IEC CD10118-2"InformationTechnology-Security Techniques-Hash-Functions:Part2:Hash-functions using. It is detailed to an n-bit block cipher algorithm", 2ISO/IEC9797, etc.
[0080]Next, in Step 1813, encryption:e Act as the plaintext message 602 and the attestation

child 603 who show drawing 14 (a) temporarily using symmetrical cryptosystem encryption / decoding processing 504 using a key, and let an encryption result be the encryption data C. Here, a message turns into the plaintext message 602 and MAC serves as the attestation child 603. Next, in Step 1814, a key is encryption:e Used as the ICC individual key 312 peculiar to IC card ID311 using symmetrical cryptosystem encryption / decoding processing 504, and this is set to enciphered-key-data K temporarily.

[0081]Enciphered-key-data K and the encryption data C are sent to IC card 201 in the form of drawing 14 (b) via the mounted vessel 211 from the road-side machine 221. Card ID which is a transmission destination, road-side machine ID which is transmitting agencies, or information and an address which are equivalent to them set to the header 611 in a figure. The encryption data C is set to the cryptogram data 612, and enciphered-key-data K is set to the key information 614.

[0082]Thus, according to this embodiment, generation of an encryption message and attestation child MAC is performed temporarily [same] using a key, using ISO/IEC9797 as a generation method of MAC.

[0083]In employing an authentication system with the gestalt which notifies information required of the IC card side mentioned later in order to calculate MAC from a key and a message temporarily, including MAC initial value etc., to IC card 201 from the road-side machine 221, Transfer of this information adds the attestation child 623 who set up this information to the form of drawing 14 (b), and it is made to transmit to it, as shown in drawing 14 (c).

[0084]On the other hand, in Step 1801, using the ICC individual key 312 peculiar to card ID311, IC card 201 decoding:d Carries out enciphered-key-data K of received data by symmetrical cryptosystem encryption / decoding processing 303, and acquires a key temporarily. decoding:d Next, carry out the encryption data C of received data by symmetrical cryptosystem encryption / decoding processing 303 in Step 1802 temporarily using a key.

[0085]and -- using a key like Step 1812 in Step 1803 from the message decoded at Step 1802 the attestation child generation processing 305 and temporarily -- MAC -- ' -- it generating and in Step 1804, It checks that MAC which is a decoding result of Step 1802 and MAC[which was generated at Step 1803]' are equivalent, if equivalent, it will progress to Step 1805, if not equivalent, it will judge that the message may be changed, and processing is interrupted in Step 1806.

[0086]Next, MAC acquired previously is added to the response data which expresses receipt of a message with Step 1805, it enciphers using the ICC individual key 312 by symmetrical cryptosystem encryption / decoding processing 303, the cryptogram C2 is made, and it transmits to the road-side machine 221 from IC card 201.

[0087]In the road-side machine 221, in Step 1815, C2 is decoded for received data using the ICC individual key 312 by symmetrical cryptosystem encryption / decoding processing 503, MAC is acquired, and it checks that it is the same as that of MAC of Step 1812.

[0088]And if it is able to check, this will check that it is a right response to encryption message C which transmitted. It is also possible to match the response C2 which transmits at Step 1805 with encryption message C which received at Step 1801 by creating MAC of response data by making MAC which received into an initial value.

[0089]It is **, and when applying the procedure of drawing 13 to the encryption communication between the road-side machines 221 of exit tollgate installation from the road-side machine 221 installed into the utilized route, since real time communication cannot be performed among both, Steps 1805 and 1815 are not performed. When applying to the encryption communication between IC card 201 and the road-side machine 221 and it does not have the ability to communicate in the road-side machine 221 and real time at IC card 201, it may not be made not to perform Steps 1805 and 1815.

[0090]Here, it explains taking the case of a message including the pass data which notifies an example of the message sent and received by processing of drawing 13 to IC card 201 from the road-side machine 221 installed into the utilized route.

[0091]The data configuration of a message is shown in drawing 15.

[0092]Among a figure, in the installation point of the road-side machine 221 with which the pass data 1701 notified the pass data concerned as mentioned above, it expresses, a car is accumulated [alias ********] in IC card 201 as channel information, and settlement processing is eventually performed by the road-side machine 221 of exit tollgate installation based on this channel information.

[0093]Next, the counter 1702 shows the counter value 317 notified from IC card 201. However, in [this message is sent to IC card 201 here from the road-side machine 221 installed into the utilized route after the authenticating processing of drawing 5 about the road-side machine 221 installed into the utilized route, and] this authenticating processing, The counter value 317 shall be notified to the road-side machine 221 which was included in the signature C1 and installed into the utilized route from IC card 201.

[0094]Here, the counter value 1702 takes the value same from the use start of a toll road to completion of settlement processing as mentioned above, and when settlement processing is completed, it is updated by the following counter value. Therefore, a counter value is data in which the 1-time nature of dealings is shown.

[0095]Next, the consecutive numbers of a message are set to the sequential number 1703. It is the consecutive numbers to the pass data set even to the exit from the entrance, and, specifically, this guarantees continuity. However, these consecutive numbers set up what took and managed cooperation between each road-side machine 221, for example, or set it up in response to the reception times of pass data from IC card 201 to last time.

[0096]Finally, the signature 1704 is an electronic signature to the pass data 1701, the counter value 1702, and the sequential number 1703 generated by the road-side machine peculiar secret key 514 of the road-side machine 221 installed into the utilized route, and the asymmetric cipher system encryption / decoding processing 503. However, it may be made to encipher the pass data 1701, the counter value 1702, and the sequential number

1703 with the encryption key which only each road-side machine 221 of installation among a utilized route and each road-side machine 221 of exit tollgate installation know instead of including a signature in a message. In this case, each road-side machine 221 manages this encryption key that only the road-side machine 221 knows.

[0097]According to such a message, the continuity of the pass data accumulated from a counter and consecutive numbers as the 1-time nature of dealings of sets of the pass data accumulated as channel information and channel information can be guaranteed, and unjust substitution of the pass data in channel information or channel information can be prevented. It may be made for the hash value of the message of pass data notified to IC card 201 from the road-side machine 221 which should just be the information which can guarantee the continuity of pass data, for example, was installed into the utilized route by last time to be used for consecutive numbers as each consecutive numbers.

[0098]The forgery of channel information by the side of IC card 201 and the mounted vessel 211 can be prevented by the signature 1704 or encryption of the pass data 1701, the counter value 1702, and the sequential number 1703.

[0099]In the above, a 1st embodiment of this invention was described.

[0100]Hereafter, a 2nd embodiment of this invention is described.

[0101]The composition of IC card 201 concerning a 2nd embodiment, the mounted vessel 211, and the road-side machine 221 is the same as that of IC card 201 concerning a 1st embodiment shown in drawing 1, the mounted vessel 211, and the road-side machine 221. The contents stored in the storage device 203 of IC card 201, The contents which are the same as the contents stored in the memory 203 shown in drawing 2 in said 1st embodiment, and are stored in the storage device 213 of the mounted vessel 211, It is the same as the contents stored in the memory 213 shown in drawing 3 in said 1st embodiment, and the contents stored in the storage device 223 of the road-side machine 221 are the same as the contents stored in the memory 233 shown in drawing 4 in said 1st embodiment in a 2nd embodiment.

[0102]Now, a 2nd embodiment adds the processing which carries out mutual recognition to IC card 201 between the road-side machines 221 to the authenticating processing of drawing 5 shown by said 1st embodiment, as shown in drawing 16. It is made to carry out by doubling the settlement processing mentioned above during the authenticating processing between three persons of IC card 201, the mounted vessel 211, and the road-side machine 221 who showed this drawing 16.

[0103]Namely, first in [in / at a 2nd embodiment / authenticating processing] Step 2102 of IC card 201, and Step 2112 of the mounted vessel 211, The certification information for road-side machine 221 of IC card 201, the mutual recognition of the mounted vessel 211, and IC card 201 from IC card 201 to the mounted vessel 211 is transmitted.

[0104]Next, in Step 2103 of IC card 201, and Step 2113 of the mounted vessel 211, the channel information for road-side machine 221 of IC card 201 from the IIC card 201 to the mounted vessel 211 is transmitted. Channel information expresses the utilized route of the toll road of the car in which the mounted vessel 211 with which IC card 201 was inserted was carried as mentioned above.

[0105]Next, in Step 2115 of the mounted vessel 211, and Step 2125 of the road-side machine 221 of exit tollgate installation, Transmission of the mutual recognition of the mounted vessel 211 and the road-side machine 221 of exit tollgate installation, the certification information for road-side machine 221 of IC card 201 from the mounted vessel 211 to the road-side machine 221, and channel information is performed.

[0106]And in Step 2106 of IC card 201, and Step 2126 of the road-side machine 221 of exit tollgate installation, According to IC card 201, the mutual recognition of the road-side machine 221, and the channel information sent via the mounted vessel 211 from IC card 201, the road-side machine 221 is made to perform the settlement of accounts which charges IC card 201.

[0107]In the above authenticating processing, Step 2115 of the mounted vessel 211, Step 2125 of the road-side machine 221 of exit tollgate installation and Step 2106 of IC card 201, and Step 2126 of the road-side machine 221 of exit tollgate installation, What is necessary is just to perform Step 2102 of IC card 201, and Step 2112 of the mounted vessel 211 in advance of this at least, when IC card 201 is inserted in the mounted vessel 211 although it is necessary to perform a part of the processing when a car passes through a tollgate exit. What is necessary is just to perform Step 2103 of IC card 201, and Step 2113 of the mounted vessel 211 at any time, when channel information is updated. Here, the channel information just specifies the grade course which can compute the utilization charge of a toll road as mentioned above, and it is sufficient if the updating is performed only at the time of toll road entrance passage and junction passage.

[0108]Since it carries out by doubling settlement processing in authenticating processing in a 2nd embodiment, unlike said 1st embodiment, settlement processing is not performed as separately as the authenticating processing of drawing 16.

[0109]Next, the details of each step of the authenticating processing shown in drawing 16 are explained.

[0110]First, Step 2102 of IC card 201 of drawing 16 and Step 2112 of the mounted vessel 211 are explained.

[0111]The details of these steps are shown in drawing 17.

[0112]If IC card 201 is inserted so that it may illustrate, the mounted vessel 211 will generate random number Ra, and will transmit mounted vessel ID411 which is an identifier peculiar to random number Ra and the mounted vessel 221 to IC card 201.

[0113]In Step 2702, IC card 201 enciphers the data for C1 creation using symmetrical cryptosystem encryption / decoding processing 303 with the ICC individual key 312, and generates the cryptogram C1. The data for C1 creation sets the ICC certificate 315 as the ICC certificate 21302 shown in drawing 18, and sets the value of the counter 317 as the counter 21303. The card ID311 grade which are a time stamp and an identifier peculiar to ICC may be set to the data for C1 creation like a 1st embodiment. A time stamp gives time information to IC card 201 from the mounted vessel 211, using the value of the timer with which the inside of an IC card was equipped, and it may be made for this to be used for it as a time stamp by IC card 201.

[0114]Next, in Step 2703, IC card 201 carries out signature processing of the data for C2 creation by asymmetric cipher system encryption / decoding processing 304 using ICC proper secret key 313:SICC which is a secret key of the asymmetry system code of IC card 201, and generates the signature C2. the data for C2 creation -- random number Ra is set as the random number 21103, and the cryptogram C1 is assigned to the attestation side intrinsic identification child 21102 of drawing 19 for mounted vessel ID411 at the signature 21104 of the ICC certificate.

[0115]Next, IC card 201 generates the random number Rb, and transmits the cryptogram C1, the signature C2, card ID (ICCID), the generated random number Rb, and the attested ICC peculiar public key 314 to the mounted vessel 211. Here, the card ID311 grade which are a time stamp and an identifier peculiar to ICC may be set to the data for C2 creation like the data for C1 creation. However, when a time stamp is included, a time stamp is also sent with the signature C2.

[0116]The mounted vessel 211 which received these verifies the justification of the attested ICC peculiar public key 314 in Step 2712 using the public key of a certificate authority, Verified ICC peculiar public key :P ICC is used and the signature C2 verifies whether the signature C2 generated or received is proper as a signature to the data for creation by asymmetric cipher system encryption / decoding processing 404.

[0117]Next, in Step 2713, the mounted vessel 211 will progress to Step 2715, if the verification result of the signature C2 is O.K., and if it is not O.K., it will stop processing in Step 2714. In the case of the stop of processing, display that on the screen of the mounted vessel 211, it announces with a sound, or the ICC card 201 is discharged from the mounted vessel 211, for example.

[0118]The mounted vessel 211 generates the signature C3 of the data for C3 creation by asymmetric cipher system encryption / decoding processing 404 in Step 2715 using mounted vessel proper secret key 413:SOBE which is a secret key of the asymmetry system code of the mounted vessel 211. the data for C3 creation -- card ID311 is assigned to the attestation side intrinsic identification child 21202, and the random number Rb is set as the time stamp 21201 of drawing 20 for execution time T3 of Step 715 at the random number 21203.

[0119]And the mounted vessel 211 transmits the signature C3, time stamp T3, and the attested mount machine peculiar public key 414 to IC card 201.

[0120]In [IC card 201 receives the signature C3, and] Step 2704, It verifies that the attested mount machine peculiar public key 314 received first is correctly attested by the certificate authority using the public key 316 of a certificate authority, ICC public key which checked what is attested correctly and verified :P OBE is used and it is verified by asymmetric cipher system encryption / decoding processing 304 whether the signature C3 is proper as a signature of the data for C3 creation generated or received.

[0121]And in Step 2705, if a verification result is O.K., processing will be ended, and if it is not O.K., processing will be stopped in Step 2706. That is told to the mounted vessel 211, and make the mounted vessel 211 display that on a screen, it is made to announce with a sound, or is made to discharge the ICC card 201 from the mounted vessel 211 in the case of a stop. Of course, as long as IC card 201 is equipped with the output device, it may be made to perform a display and an announcement from the output device.

[0122]Next, the details of Step 2115 of the mounted vessel 211 of drawing 16 and Step 2125 of the road-side machine 221 of exit tollgate installation are explained.

[0123]A procedure with these detailed steps is shown in drawing 21.

[0124]First, the road-side machine 221 generates the random number R4, and transmits road-side machine ID511 and the random number R4 which are an identifier of the road-side machine 221 to the mounted vessel 211.

[0125]In Step 2802, using the mounted vessel individual key 312, the mounted vessel 211 enciphers the data for C4 creation using symmetrical cryptosystem encryption / decoding processing 403, and generates the cryptogram C4. The data for C4 creation the random number R5 generated to random number (1) 1401 of drawing 11 of drawing 11, Random number (2) The cryptogram C1 is set as the signature 1405 for card ID (ICCID) which received the random number R4 received from the road-side machine 211 to 1402 to the attestation side identifier 1403, and received road-side machine ID from IC card 201 to the ICC identifier 1404.

[0126]And the mounted vessel 211 transmits cryptogram C4 and mounted vessel ID411 to the road-side machine 221 with the channel information received from IC card 201 at Steps 2103 and 2113 of drawing 16.

[0127]the road-side machine 221 is individual in Step 2812 from mounted vessel ID411 which received, and the mounted vessel individual key generation key 513 -- by key generation processing 505:f, it generates, and using the generated mounted vessel individual key, the mounted vessel individual key 412 is decoded cryptogram C4, and is verified by symmetrical cryptosystem encryption / decoding processing 503. Here, a verification result will be judged to be O.K. if the random number R4 and road-side machine ID which the road-side machine 221 transmitted previously are able to be checked.

[0128]In Step 2815, the road-side machine 221 will progress to Step 2813, if a verification result is O.K., and if it is not O.K., in Step 2816, it will stop processing. In this case, display that on the screen of the road-side machine 221, it is announced with a sound, or is told to the mounted vessel 211. Display the mounted vessel 211 told this purport on the screen of the mounted vessel 211, it is announced with a sound, or discharges the ICC card 201 from the mounted vessel 211.

[0129]Next, in Step 2813, the road-side machine 221 enciphers the data for C5 creation by symmetry system cryptosystem encryption / decoding processing 514 using the mounted vessel individual key restored previously, creates the cryptogram C5, and transmits to the mounted vessel 211. The data for C5 creation sets the random number R5 as the random number 1501 shown in drawing 12, sets the random number R4 as the random number 1502, and sets mounted vessel ID to the attestation side identifier 1503.

[0130]And the road-side machine 221 transmits the cryptogram C5 to the mounted vessel 211.

[0131]In Step 2803, the mounted vessel 211 will decode and verify the cryptogram C5 by symmetrical cryptosystem encryption / decoding processing 403 using the mounted vessel individual key 413, if the cryptogram C5 is received. Here, a verification result will be judged to be O.K. if R5 and mounted vessel ID411 which the random number R4 which the mounted vessel 211 received previously, and the mounted vessel 211 generated are able to be checked.

[0132]In Step 2804, the mounted vessel 211 will end processing, if a verification result is O.K., and if it is not O.K., in Step 2805, it will stop processing. In the case of a stop, tell an attestation failure to the road-side machine 221, display on the screen of the mounted vessel 211, it announces with a sound, or IC card 201 is discharged from the mounted vessel 211.

[0133]Next, the details of Step 2106 of IC card 201 of drawing 16 and Step 2126 of the road-side machine 221 of exit tollgate installation are explained.

[0134]A procedure with these detailed steps is shown in drawing 22.

[0135]First, card ID which received the road-side machine 221 in Step 2912, individual using the ICC individual key generation key 512 -- the ICC individual key 312 is generated by key generation processing 505:f, using the generated ICC individual key 312, it decodes cryptogram C1 by symmetrical cryptosystem encryption / decoding processing 503, the ICC certificate 315 is taken out, and this is verified. The check of the ICC certificate 315 is performed according to the kind of certificate. Here, since the ICC certificate is attested by the certificate authority 331, it verifies by asymmetric cipher system encryption / decoding processing 504 using the public key 517 of a certificate authority. Or when [which the ICC certificate 315 attested beforehand with the road-side machine peculiar secret key 514 of the road-side machine 221] a basis is carried out, it verifies by the road-side machine peculiar public key 515 of the road-side machine 221.

[0136]Next, in Step 2913, the road-side machine 221 will progress to Step 2915, if the verification result of Step 2912 is O.K., If it is not O.K., processing is stopped, the attestation failure of IC card 201 in the road-side machine 221 will be told to the mounted vessel 211, and the mounted vessel 211 will be made to display that on a screen, to make it announce with a sound, or to discharge IC card 201 from the mounted vessel 211 in Step 2914.

[0137]Now, in Step 2915, the road-side machine 221 enciphers the data for C6 creation with the ICC individual key 312, and creates the cryptogram C6. The data for C6 creation card ID which received to the attestation side identifier 21600 shown in drawing 23, The settlement data which shows the fee etc. of the toll road computed from the channel information which passed the road-side machine certificate 516 to the road-side machine certificate 21602, passed the mounted vessel 211 to the settlement data 21615, and obtained the time information of the road-side machine 221 to the time stamp 21601 is set up. The signature by the side of a road-side machine may be added to settlement data. Setting out of the road-side machine certificate 516 may be omitted.

[0138]The road-side machine 221 transmits the cryptogram C6 to IC card 201 via the mounted vessel 211. At this time, the mounted vessel 211 transmits the received cryptogram C6 to IC card 201 as it is.

[0139]In Step 2902, IC card 201 decrypts the received cryptogram C6 using symmetrical cryptosystem encryption / decoding processing 303 with the ICC individual key 312, and takes out and verifies the road-side machine certificate 515. The check of the road-side machine certificate 515 is performed according to the kind of certificate. Here, a road-side machine certificate is attested by the certificate authority 331, and is verified by asymmetric cipher system encryption / decoding processing 304 using the public key 316 of a certificate authority.

[0140]Next, in Step 2903, if IC card 201 is judged to be the verification O.K., it will check the contents of settlement data and will end processing. If it is not O.K., processing is stopped, settlement of accounts will be made abortive and IC card 201 will be made to notify that to the mounted vessel 211 or the road-side machine 221, to display on the screen of the mounted vessel 211, to announce with a sound, or to discharge from the mounted vessel 211 in Step 2905.

[0141]by the above, the road-side machine 221 verifies the justification of IC card 201 and the mounted vessel 211, and the mounted vessel 211 verifies the justification of IC card 201 and the road-side machine 221 -- it means that IC card 201 had completed verification of the justification of the mounted vessel 211 and the road-side machine 221

[0142]Here, the ICC certificate 315 of drawing 18 is the data attested by the certificate authority, is having enciphered with the key sharable only by IC card 201 and the road-side machine 221, and serves as data which can verify only the road-side machine 221. However, this may use the ICC certificate 315 as the data beforehand signed with the road-side machine peculiar secret key 514 which is a secret key of an asymmetric cipher system peculiar to the road-side machine 221. In that case, in Step 912, the ICC certificate 315 is verified by asymmetric cipher system encryption / decoding processing 504 using the road-side machine peculiar public key 515. The same may be said of the road-side machine certificate 516.

[0143]In the above, a 2nd embodiment of this invention was described.

[0144]The authenticating processing in a 2nd embodiment may be corrected to the gestalt which performs as follows mutual recognition which used the random number between IC card 210 and the road-side machine 221.

[0145]Namely, first as data for C1 creation used at Step 2702 of drawing 17, What set the random number Ricc which generated the value of the counter 317 for the ICC certificate

315 by the IC card at the counter 21313 at the random number 21314 as the ICC certificate 21312 which was replaced with the thing of drawing 18 and shown in drawing 24 is used.
[0146]It replaces with the procedure of Step 2106 of IC card 201 of drawing 16 shown in drawing 22, and Step 2126 of the road-side machine 221 of exit tollgate installation, and the procedure shown in drawing 25 is used.
[0147]That is, as mentioned above, if the road-side machine 221 verifies the ICC certificate, it will transmit the cryptogram C8 which enciphered the data for C8 creation with the IC card individual key generated at Step 2912 to IC card 201 via the mounted vessel 211. The data for C8 creation sets up card ID(ICCID) 311 which received to the attestation side identifier 21610 shown in drawing 26, Set the time information of the road-side machine 221 as the time stamp 21611, and the road-side machine certificate 516 is set as the road-side machine certificate 21612, Random number (1) The random number Ricc decoded by 2912 from StepC1 is set as 21613, and settlement data is set as the settlement data 21615 for the random number Rrse which the road-side machine 221 generated to random number (2) 21614.
[0148]IC card 201 decrypts and verifies the cryptogram C8 by symmetrical cryptosystem encryption / decoding processing 303 in Step 21002 using the ICC individual key 312. And in Step 21003, the random number Ricc which IC card 201 transmitted previously, card ID311, or a road-side machine certificate is verified, If justification is able to be checked, will judge the road-side machine 221 to be a just partner, and it progresses to Step 21006, If justification cannot be checked, processing is stopped in Step 21005, settlement data is canceled and IC card 201 is made to notify that to the mounted vessel 211 or the road-side machine 221, to make it display on these screens, to make it announce with a sound, or to discharge from the mounted vessel 211.
[0149]On the other hand, in Step 21006, IC card 201 enciphers the data for C9 creation by symmetry system cryptosystem encryption / decoding processing 303 using the ICC individual key 312, creates the cryptogram C9, and transmits to the road-side machine 221 via the mounted vessel 211. The data for C9 creation sets the random number Ricc as random number (2) 21502 for the random number Rrse random number (1) 21501 shown in drawing 27, and sets card ID311 to the attestation side identifier 21503.
[0150]In Step 21016, the road-side machine 221 will be decoded and verified by symmetrical cryptosystem encryption / decoding processing 503 using the ICC individual key 312 which generated the cryptogram C9 at Step 2912, if the cryptogram C9 is received.

[0151]And in Step 21017, if the road-side machine 221 is able to check the random number Rrse which the road-side machine 221 transmitted previously, an IC card will judge it to be a just partner, it ends processing, and if it is not O.K., it will stop processing in Step 21018. In the case of a stop, an attestation failure is told to IC card 201, and it cancels settlement processing while IC card 201 displays that on the screen of the mounted vessel 211, or is made to announce with a sound, or makes IC card 201 discharge from the mounted vessel

211 and carries out slack.

[0152]In the above gestalt, since fixed mutual recognition of IC card 201 and the road-side machine 221 can be performed by the random number Rrse and the random number Ricc, It may be made to omit the both sides or one side of including an IC card certification in the data for C1 creation, and including a road-side machine certificate in the data for C8 creation.

[0153]Also in a 2nd embodiment, it carries out like said 1st embodiment about renewal of the channel information stored in the memory 211 of IC card 201. Also in a 2nd embodiment, the same encryption communication of said 1st embodiment also performs the notice of the information on the notice of pass data, the notice of the channel information mentioned above, the settlement data performed for the settlement processing mentioned above to accumulate, etc. performed between IC card 201 and the road-side machine 221.

[0154]Since attestation and processing of the settlement of accounts between a road side device and an IC card, etc. are performed [according to a 2nd embodiment described above] in parallel in addition to the effect of said 1st embodiment, even if a car passes through a tollgate at a high speed more nonstop, it is expectable that the both sides of attestation and settlement of accounts can be performed properly. Mutual recognition between IC cards 201 of the road-side machine 221 is also realized.

[0155]in addition -- setting to each attestation, although the symmetrical cryptosystem is used by attestation between IC card mount machines at an above embodiment [1st and 2nd] by attestation between an asymmetric cipher system and a mounted vessel-road-side machine, and attestation between IC card road-side machines -- a symmetrical cryptosystem and asymmetric cipher system -- whichever may be used.

[0156]The ICC certificate 315 mentioned above may be the data which can create only the road-side machine 221 prepared beforehand, for example, the data signed with the road-side machine peculiar secret key 514 which is a secret key of a peculiar asymmetric cipher system of the road-side machine 221. The processing which enciphers this with the common key of IC card 201 and the road-side machine 221 well also as C1 as it is in this case for C1 creation may be omitted. Verification of the 221 road-side machineC1 verifies the ICC certificate 315 using the road-side machine peculiar secret key 514 and the corresponding attested road-side machine peculiar public key 515.

[0157]Or the data which can create only IC card 201 which prepared the road-side machine certificate 516 beforehand, For example, it is considered as the data signed with the ICC peculiar secret key 313 which is a secret key of a peculiar asymmetric cipher system of IC card 201, and may be made to send to IC card 201, without enciphering from the road-side machine 221. In this case, IC card 201 verifies the road-side machine certificate 516 for the received road-side machine certificate 516 using the attested ICC peculiar public key 314.

[0158]

[Effect of the Invention]As mentioned above, according to this invention, when

communication between 2 devices used as the attestation side device and an attesting side device is performed via the 3rd device, in the attestation side device, the authentication system which can attest an attesting side device with high reliability can be provided.
[0159]When communication between 2 devices is performed via the 3rd device, even if the hour corresponding given to communication between the 3rd device and one device is a short time, the authentication system which can perform attestation between 2 devices which communicate via the 3rd device can be provided.

[Translation done.]